3. Time to make hackers cry – let's scan smart and secure hard!

In this task, you'll harness the power of the Nmap Scripting Engine `NSE` to perform a comprehensive security analysis of a target network

Write `a bash script` that performs the following tasks:

- Your script should accept `a host` as an arguments `$1`.
- Use multiple NSE scripts **sequentially** to perform a comprehensive security analysis, including:
  - `http-vuln-cve2017-5638` for the Apache Struts 2 vulnerability.
  - `ssl-enum-ciphers` to enumerate supported SSL/TLS ciphers.
  - `ftp-anon` to check for anonymous FTP login.
- Save the output to `comprehensive_scan_results.txt` for later analysis.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x07nmappostportscan_scripting]
└─🏴 sudo ./3-comprehensive_scan.sh scanme.nmap.org
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-20 10:31 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.45s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f



PORT      STATE  SERVICE
21/tcp    closed ftp
22/tcp    open   ssh
80/tcp    open   http
443/tcp   closed https
9929/tcp  open   nping-echo
31337/tcp open   Elite
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.04 seconds
```

The command:

```
nmap --script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon $1 -oN
comprehensive_scan_results.txt
```

Explanation:

1. `nmap`:
   - Runs the Nmap network scanner.
2. `--script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon`:
   - This option specifies that multiple **NSE scripts** should be used in the scan:
     - `http-vuln-cve2017-5638`: Checks for the **CVE-2017-5638** vulnerability in Apache Struts, which is a remote code execution vulnerability.
     - `ssl-enum-ciphers`: Enumerates and lists the supported **SSL/TLS ciphers** on the target, helping you assess the security of the encryption in use.
     - `ftp-anon`: Checks whether the FTP server allows **anonymous login** without authentication, which could pose a security risk.
3. `$1`:
   - Represents the **target IP address** or **hostname**. This is a positional parameter in a script, so it will be replaced with the target when the script is run.
   - Example: If `$1` is replaced with `192.168.1.10`, the full command becomes:

     ```
     nmap --script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon
     192.168.1.10 -oN comprehensive_scan_results.txt
     ```
4. `-oN comprehensive_scan_results.txt`:
   - Directs Nmap to save the results of the scan in **normal output format** to a file named `comprehensive_scan_results.txt`.

How It Works:

- Nmap performs a scan against the target (`$1`) using the following scripts:
  1. `http-vuln-cve2017-5638`: Checks if the Apache Struts server is vulnerable to CVE-2017-5638.
  2. `ssl-enum-ciphers`: Lists the supported SSL/TLS ciphers on any service running SSL (e.g., HTTPS or FTPS) and checks if any insecure ciphers are used.
  3. `ftp-anon`: Tests whether an FTP server allows anonymous login, which can expose sensitive data.

- The results are stored in `comprehensive_scan_results.txt`.

Example Usage:

Assume you want to scan the target `192.168.1.10`:

```
nmap --script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon 192.168.1.10
-oN comprehensive_scan_results.txt
```

Sample Output in `comprehensive_scan_results.txt`:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-28 15:00 UTC
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).

PORT    STATE SERVICE
80/tcp  open  http
| http-vuln-cve2017-5638:
|   VULNERABLE:
|   Apache Struts CVE-2017-5638 Remote Code Execution
|     State: VULNERABLE
|     Exploitability: High
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
|       https://nvd.nist.gov/vuln/detail/CVE-2017-5638
|
|_  Affected versions: Apache Struts 2.3.5 to 2.3.31, 2.5 to 2.5.10

443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       0x0035 (ECDHE-RSA-AES256-GCM-SHA384)
|       0xC02F (ECDHE-RSA-AES128-GCM-SHA256)
|     ...
|   SSLv3:
|     ciphers:
|       0x0035 (AES256-SHA)
|_    Insecure ciphers found

21/tcp  open  ftp
| ftp-anon:
|   Anonymous FTP login allowed (no password)
|     - Directory listing is possible
|     - Potential risk of unauthorized file access
|_  FTP server allows anonymous login

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
```

What You Learn From This Output:

1. **CVE-2017-5638 Vulnerability**: The Apache Struts service on port 80 is vulnerable to a remote code execution vulnerability, which can be exploited by an attacker.
2. **SSL/TLS Cipher Information**: The server supports insecure SSL/TLS ciphers, making it vulnerable to attacks like **BEAST** or **POODLE**. It's important to disable insecure ciphers and prefer stronger ones (e.g., `ECDHE-RSA-AES256-GCM-SHA384`).
3. **FTP Anonymous Login**: The FTP service on port 21 allows anonymous login, which poses a security risk as unauthorized users can access sensitive files.

Benefits:

- **Comprehensive Security Assessment**: The command checks for a wide range of potential vulnerabilities on the target, including web application flaws, SSL/TLS weaknesses, and misconfigured FTP services.
- **Easy Reporting**: Outputting to a file (`comprehensive_scan_results.txt`) allows you to review and share findings with others.

Limitations:

- **False Positives/Negatives**: Depending on the configuration and detection methods, the script may report false positives or fail to detect vulnerabilities in non-standard configurations.
- **Target-Specific**: The scripts are tailored for specific vulnerabilities or configurations, so they may not catch other types of issues present on the target.

Improvement Suggestions:

- Combine additional vulnerability checks to expand your scan:

  ```
  nmap --script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon,vuln $1 -oN comprehensive_scan_results.txt
  ```

- Use output options like **XML or JSON** for structured results, which can be processed by other tools:

  ```
  nmap --script=http-vuln-cve2017-5638,ssl-enum-ciphers,ftp-anon $1 -oX vuln_scan_results.xml
  ```